美国国家计算机

安全中心

理解自动化信息系统中数据残留的指南

（中文版**v1.00**）

翻译：陈海燕，CISSP（phrackchen@hotmail.com）



华安信达

NCSC-TG-025
Library No. 5-236,082
第二版

1991年9月

序

国家计算机安全中心发表了《理解自动化信息系统中数据残留的指南》一文，它是我们技术指导方针项目产品“彩虹系列”文档的一部分。在彩虹系列中，我们详细讨论了《国防部受信计算机系统评测标准》（DoD 5200.28-STD）的特性并为满足其各项需求提供指导。国家计算机安全中心通过其受信产品评测项目评测商业计算机系统产品的安全特性。这些项目共同确保机构具备保护其受信计算机系统中重要数据的能力。虽然数据残留不是受信计算系统的一项直接评测标准，但是它对于保护受信计算系统所使用的信息具有至关重要的意义。

《理解自动化信息系统中数据残留的指南》的主要读者对象是负责对敏感或保密的自动化信息系统中内存和第二存储器进行安全处理的人员。这些人员应该了解这些介质的记忆特性、在擦除和释放过程中的已知风险，以及协助防止敏感或保密信息泄漏的得到认可的安全规程。本版本替代了1985年11月15日发表的CSC-STD-005-85，《国防部磁性残留安全指导方针》。

做为国家计算机安全中心的主任，我邀请您为本技术指导方针的修订提出建议。我们计划定期或在需要时对本文进行审查。

美国国家计算机安全中心
主任
Patrick R. Gallagher, Jr.
1991年9月

致谢

国家计算机安全中心特别感谢本指导方针的主要作者，美国空军的James K. Goldston上尉及其为本文所进行的技术支持和准备工作。我们感谢许多参与本文准备工作的人们。他们的详尽检查和建议的是非常宝贵的。国家计算机安全中心感谢Bane W. Burnham博士和David N. Kreft，没有他们的努力修订版是无法问世的。其他提供宝贵意见的审核人员是Carole S. Jordan、Lawrence M. Sudduth，以及Kim Johnson-Braun和George L. Cipra。

内容目录

1 介绍

数据残留是数据在被以某种形式擦除后所残留的物理表现。存储介质被擦除后可能留有一些物理特性使数据能够被重建。本文讨论出于重用或释放目的进行存储介质擦除时数据残留所扮演的角色。

各种已发表的文献详细描述了清理、净化、撤销密级或销毁自动化信息系统（AIS）存储介质的规程。［1、2、4、5、6、8、9、13和16］国防部（DoD）于1972年和1973年分别发表了国防部指令5200.28，《自动化信息系统的安全需求》［17］及其对应的安全手册5200.28-M，《自动化数据处理安全手册》。［1］这两个文献于1979年得到了修订以回应国防科学委员会项目组关于建立计算机安全需求、控制和措施的国防部统一政策的建议。指令在1988年3月又得到了修订，修订手册的工作也在进行中。

国防部5200.28-M涉及到安全处理和处置内存和第二存储器的国防部需求。国防部要求各部门使用DoD 5200.28指令和DoD 5200.28-M，国防部门负责人还可以通过提供更详细的、与这些政策相一致的指导方针和说明来增强这些需求以满足其需要。参与国防工业安全项目（DISP）的国防部承包商和分包商被要求执行DOD 5220.22-M，《保护保密信息的工业安全手册》。［8］国防调查局负责颁布体现DoD 5220.22-M的政策。与这些政策文献不同的是，《理解自动化信息系统中数据残留的指南》不提出需求。

在AIS生命周期的某些时刻，其主存储器和第二存储器可能需要被重用、撤销密级、销毁或释放。对于安全官员、计算机操作员和其它用户或AS资源监护人来说，了解AIS存储介质重用、撤销密级、销毁和释放的风险是非常重要的。他们还应该了解更改AS存储介质敏感级别或将应用中的介质转移到安全条件相对较低环境中的固有风险。他们应该使用适当的规程防止此类介质中所包含敏感信息的可能泄漏。（本文中的“敏感”是指保密和非保密但敏感的信息。）本文中的规程和指导方针基于研究、调查结果、当前政策和日常实务。

本指导方针被分为以下章节：第2章提供使用本指导方针的信息并介绍国防部使用的术语。第3章讨论消磁器的使用和消磁器产品清单（DPL），即通过国防部评测的消磁器清单。第4章“风险考虑因素”中除了4.2节“受热和使用年限的影响”有改动以外，其它内容与本文第一版相同，另外还有覆盖和消磁方面的附加信息。第5章涉及到国防部认可的擦除标准。最近出现的存储技术和磁盘练习器在第6章中讨论。第7章涉及需要进一步研究的领域并提供与剩磁相关的磁介质技术的附加信息。

1.1 目的

本出版物的目的在于为负责安全处理敏感AIS内存和第二存储器的人员提供信息。（本指导方针也适用于任何电或磁存储介质，如仪器设备使用的磁带。）本指导方针提供与大多数AIS存储介质的清理、净化、撤销密级、销毁和释放相关的信息。

虽然数据残留不是受信计算系统的一项直接评测标准，但是它对于保护受信计算系统所使用的信息具有至关重要的意义，因此，在国家计算机安全中心（NCSC）指导方针中加以论述。NCSC之所以发表此文是因为使用受信计算系统的机构对此信息具有一致的需求。另外，读者应该注意到这只是一个指导方针而不应被用以替代政策。

1.2 历史

因AIS存储介质的记忆特性造成的问题（即数据残留）早在1960年就被认识到了。如果不执行数据清除规程，在存储介质被释放到非受控环境时就可能无意中造成敏感信息的泄漏。消磁、覆盖、数据加密和介质销毁是一些被用于保护敏感信息免遭泄漏的方法。经过一段时间的应用，与AIS存储介质清理和净化相关的具体实务逐渐被广泛采纳。

国防部与伊利诺伊理工学院研究所签订了一系列研究合同，并于1981年和1982年完成了这些研究项目。研究结果确认了消磁措施对于磁带介质的有效性。［19］另外，在卡耐基梅隆大学所进行的研究中，使用通信理论和设计用于探测已擦除磁盘数字信息的磁模型化实验为磁盘可擦除性提供了实验数据。［11、21和22］此项工作以及国防部还未发表的研究结果为磁盘消磁标准建立了基础。

1981年1月2日，国家安全局局长承担了国防部计算机安全的职责。因此，根据国防部指令5215.1的授权在国家安全局中建立了国防部计算机安全中心（DoDCSC）。[3]随后组成了DoDCSC标准处（现在的规范、标准和指导方针处），其工作任务是支持广泛的计算机安全相关课题。1985年，根据145号国家安全决策指令将DoDCSC更改为NCSC。［15］做为其使命的一部分，为了提供用于AIS安全运作的信息，NCSC发表了《国防部磁性残留安全指导方针》，这是本指导方针的第一版。

2 概述

应该以AIS所处理信息的最高安全级别的规定来保护AIS及其存储介质。也就是按照得到认可的净化规程处理AIS及其相关存储介质和通过管理方式撤销密级。应该持续地保证对敏感信息的保护而不将其置于可能遭到危害的环境中。信息保护者必须保护存储介质免遭两种主要威胁的攻击：键盘攻击（通过系统软件功能提取信息）和实验室攻击（通过实验室方法提取信息）。在AIS采购前就应该实施防范这些威胁的规程，并且在AIS的整个生命周期期间持续应用这些规程。

2.1 本指导方针的使用

被指定的审批机关和信息系统安全官（ISSO）可以在选择和评测清理、净化、撤销密级、或销毁AIS存储介质的方法时参考本指导方针。国防部门可以将本指导方针的信息包含在其安全培训和意识培养项目中,但是不应使用指导方针代替已有的政策。

本文中的指导方针有两种强调级别。AIS存储介质安全处理中最重要的部分使用“ISSO应该…”之类的用词。比较次要的指导性内容使用“…是很好的措施”或“可以…”之类的用词。所以，“可以”一词代表的重要性低于“应该”一词。

2.2 重要定义

本节提供了对于理解数据残留问题很重要的一些概念及其解释。在第7章后面有更全面的术语表。

清理：在处理的结束阶段清除AIS中的敏感数据，包括AIS存储设备和其它具有存储能力的外设中的，这种方式提供与数据敏感性相当的保证，即无法使用普通的系统功能，也就是通过键盘重建数据。（这可能包括使用高级的诊断功能。）在执行清理前无需将AS与外部网络断开。［1，草案］

在安全的物理环境（介质所使用的环境）得以维护时可以使用清理方式。换句话说，介质在以前所使用的同一AIS和环境中被重用。

在运行的计算机中，如果可以确信系统实施了存储空间与非受权用户的分离，则可以通过对未分配系统存储空间的覆盖完成清理。例如，在实施环境有保证的前提下，只要覆盖文件或所有系统存储一次就足以确保以前的信息无法通过键盘攻击得以重建。注意：在一些系统中简单删除文件只是清除文件指针，这种情况下通过普通的系统功能（即诊断程序）通常就可以恢复以前的信息。

净化：在处理的结束阶段清除AIS中的敏感数据，包括AIS存储设备和其它具有存储能力的外设中的，这种方式提供与数据敏感性相当的保证，即无法使用末端开放的

实验室技术重建数据。在执行净化前AIS必须与外部网络断开。［17］

在安全的物理环境没有得到维护（介质所使用的环境）时必须使用净化方式。换句话说，计划将介质从安全设施中释放到非净维护设施或类似的非安全环境时必须使用净化方式。

注意：净化的定义允许进行等级化的数据清除规程，但是当前的标准还没有利用这一特点。也就是，“在提供与数据敏感性相当的、数据无法被重建的保证条件下”清除数据，这意味着可以制定等级化应用的标准。例如，可以将标准制定为允许安全官使用80 db对保密磁带进行消磁，使用90 db对机密磁带进行消磁。但是实践表明，这不是一种可行的方案。在DoD 5200.28-M中详细描述了得到认可的清理和净化规程，在一些国防部规章中也有进一步的解释。

撤销密级：撤销相关介质保密级别的规程和管理活动。撤销密级的规程性内容实际上就是介质的净化以及清除任何表示密级的标签，也可以使用表示非保密存储介质的标签代替原来的标签。管理性内容就是通过向适当机关提交决策文书的方式撤销存储介质的密级。

无论是撤销还是降低存储介质的密级，文书都应该包括以下内容：

a. 介质的描述（类型、厂商、型号和序列号）。
b. 介质的密级以及本次活动重新评定后所要求的结果密级。
c. 净化规程的描述，如果进行消磁要包括所使用消磁器的构造、型号和序列号以及消磁器最近一次测试的日期；如果进行覆盖要包括软件的审批意见；如果净化规程不同于以前的方式应包括净化规程的描述和授权情况。
d. 执行规程和检验结果的人员姓名。
e. 降级、撤销密级或释放的原因。
f. 活动所需的数据所有者的合作情况。
g. AIS或存储介质预期的接收者或目的地。

矫顽性：使用磁场强度（Oe）为测量单位的一种磁材料的特性，是将磁感应从原来的剩余状态还原到零所需的磁场（反向）总量，也就是将介质由记录状态转换到非记录状态所需的磁场强度。矫顽性的数值由厂商或供应商提供。

I类磁带：矫顽性不超过350 Oe的磁带（也被称为低能量磁带），例如氧化铁涂层磁带。注意：矫顽性的最高值在325 Oe到350 Oe之间变化。

磁盘，也就是金属层上的氧化物微粒，也具有多种矫顽性水平。但是，研究表明磁盘的物理剩磁特性比较容易处理。因此，磁盘被当作I型磁带进行处理，后面会有更详细的论述。

II型磁带：矫顽性范围从351到750 Oe之间的磁带（也被称为高能量磁带），例如氧化铬涂层磁带。I和II型的定义很大程度上是由磁带制造业确定的。低能量磁带被最先开发出来，它们具有300 Oe ＋ 10％左右的矫顽性。第二代磁带是高能量磁带，其矫顽性在650 Oe ＋ 10％左右。 实际上不存在任何自然发生的条件用于定义II型磁带。在实际应用中，没有任何消磁器可以满足国家安全局／中央安全局（NSA/CSS）对上述II型磁带的L14-4-A规范需求。［13］

III型磁带：矫顽性高于750 Oe的磁带，例如钴铁氧化物涂层和金属微粒涂层磁带。由于提供了这一定义，所以也会论述这类介质。

消磁器：能够产生对磁存储介质进行消磁的磁场的设备。I型消磁器可以净化I型磁带和所有磁盘。II型消磁器可以净化I型和II型磁带。目前还没有III型消磁器。当前，所有I、II、III型磁带都可以使用I型消磁器进行清理。但是，可能会开发出具有更高矫顽性而无法使用I型消磁器清理的磁带。可以通过DPL来查询是否有可供使用的III型消磁器。第3章将进一步讨论消磁器。

永久磁铁消磁器：满足对软盘、盘片、磁鼓表面、磁泡记忆芯片和薄膜记忆单元消磁需求的手持式永久磁铁。它不用于磁带的消磁。

2.3 对象重用和数据残留

多用户系统的数据提取问题早在DoD 5200.28-STD《受信计算机系统评测标准（TCSEC）》［20］成为对受信系统进行评测的尺度以前就已经引起关注了。TCSEC以其需求体现了这种关注，即受信计算基（TCB）应具有执行对象重用政策的机制。这个机制必须确保用户无法使用TCB接口从循环使用的存储介质（如内存或磁盘页面）上恢复其他用户的数据。受信计算系统中的对象重用（在很大程度上）相当于“清理”。

可以实施对象重用使包含对象（文件）的地址空间在释放存储单元（最终结果是未分配地址空间得到清理）或分配存储单元（最终结果是未分配存储空间可能包含数据残留）时得到清理。（注意：还存在其它不涉及清理的实施对象重用的方法。）这样，通常就无法通过键盘从共用数据存储池中的得到其他用户的信息了。

满足对象重用需求的受信系统和只进行清理或净化的程序之间的比较已经有人作过一些，应该注意的是，覆盖程序无法得到如受信系统那样的信任。这主要是因为覆盖程序所运行的环境造成的。

设计中包含对象重用机制的受信系统得到了TCB的保护和支持，对象重用机制得到了实际的信任。商业的覆盖程序通常被设计为可以在不同的系统上运行，而不像受信系统那样得到严格的评测；尽管如此，还是应该对覆盖程序进行保护以防其遭到非法修改。这两种安全特性提供了类似的数据机密性但是他们满足不同级别的计算机

安全需求。

3 消磁器

DoD 5200.28-M要求消磁设备通过国防部门实验室或其评估测试得到认证的商业测试实验室的测试和核准。在DoD 5200.28-M中公布了测试方法和性能标准。国家安全局／中央安全局（NSA/CSS）的L14-4-A规范《磁带消磁器》［13］是DoD 5200.28-M消磁器测试需求的更新版本。NSA/CSS已经通过发布NSA/CSS L14-4-A规范确认了当前的消磁器测试标准。

3.1 基本原理

通过使被称为磁畴的极小区域更改磁取向使其处于给定磁场方向的方法在磁介质中存储数据。这种现象与指南针指向地球磁场方向是基于同样的机理。消磁，通常被称为擦除，使磁畴处于与原先无关的随机组合，从而使以前的数据无法被恢复。在消磁后有一些磁畴其磁取向没有得到随机化。这些磁畴表示的信息通常被称为剩磁。正确的消磁会确保剩磁不足以重建数据。

可以通过两种方法完成消磁方式的擦除：在交流擦除中，通过施加幅度随时间由初始高峰逐渐减小的交互场（也就是交流电）对介质进行消磁；在直流擦除中，通过施加单向场（也就是直流电或使用永久磁铁）使介质饱和。

3.2 消磁器测试

国防部采纳了国家安全局消磁设备安全标准，该标准要求消磁器将特定的最坏模式模拟测试信号降低90分贝（db）。简而言之，消磁必须将测试信号减小到初始强度的十亿分之一。但是，磁介质上记录的信号比最坏模式测试信号要容易擦除。最坏模式测试信号是使磁带磁饱和的测试信号，由参考资料1和13提出。在测试信号被记录在磁带上以后，对磁带进行消磁并对剩余的信号进行测量以检验其是否符合90db的标准。这样就测定了消磁器的效率。

3.3 标注磁带

仅从外表很难区分不同磁带的类型。因此，建议负责人员确保磁带卷在初次使用时附上类型标签（即I、II、III型）。标签应该一直贴在磁带卷上直到将磁带从磁带卷上剪除或将磁带卷消毁为止。

在有些情况下，在磁带卷上添加过多的磁带标签可能会导致操作员错误。一些设施要求安全官使用厂商标签来确定磁带的矫顽性。任何情况下都应该使用严格的物品清单控制措施来保证对磁带类型的识别以便使用正确的净化规程。

3.4 消磁器产品清单（DPL）

NSA信息系统安全产品和服务目录［10］中包括满足NSA/CSS L14-4-A规范需求的消磁器清单。目录每季度进行更新，可以通过美国政府印刷机构获得。

3.5 消磁设备故障

由于存在设备故障的可能性，应该定期测试消磁设备以便在整个设备生命周期中对操作的正确性进行检验。应该按照进度表定期进行预防性维护以排除机械或电子问题。一些厂商有维护合同和推荐的维护进度表来确保消磁规程的完整性。

为了粗略地评估消磁器的效率，可以通过使用磁强计对一些型号（由于无法接触到磁场，有些型号的I型消磁器无法采用这种方式进行测试）的I型消磁器所产生的磁场强度进行本地测试。尽管如此，还是需要更全面的测试来为消磁器的正确操作提供充足的保证。

可以通过使用以下规程定期对I型和II型消磁器进行更全面的定期测试以检验其是否满足NSA/CSS L14-4-A规范对信号强度90 db消减的需求：在磁带上预先记录特定的测试信号（在实验室中进行），对磁带进行消磁，然后将磁带送到可以测试剩余信号水平的实验室中。［13］请咨询地方权威机构或工程技术人员以确定机构是否可以得到这种服务。DPL中列出了两家公司，Integra技术公司和数据安全公司可以测试所安装的消磁器的效率。

虽然这样的定期测试不是国防部的要求，但是我们极力推荐这样做。在消磁器安装完毕后，应该在使用的前两年对其进行定期测试（每六个月至少一次）。此数据可以被用于生成消磁器使用的直方图。可以基于这一信息制定以后的测试时间间隔，如每9个月、每年、每18个月等。

注意，无论是新安装的消磁器还是使用多年的消磁器，假设其能够提供足够的擦除是错误的。依赖于国防部对消磁器厂商产品线的评估也是不谨慎的，因为存在产品故障的可能性。

4 风险考虑因素

在涉及到AIS存储介质重用和释放时应该考虑到多项风险因素。AIS安全人员、操作人员、用户和其他指定的负责人员应该在试图对存储介质撤销密级或作出释放决定前了解这些风险。

4.1 被释放介质的目的地

无论出于何种目的，当AIS存储介质被释放到控制环境以外时都会增加危及敏感数据安全的风险。

4.2 受热和使用年限的影响

本文的第一版报告了磁介质在长期存储或高温（120华氏度或以上）条件下变得难以消磁或擦除的情况。进一步的研究证实了高温和使用年限对擦除过程的影响。[14]

4.3 存储设备的机械故障

一些早期的磁盘驱动器需要人工调整读／写磁头。这种技术条件下覆盖的效率就会因设备故障或机械错误而降低，如读／写磁头的偏移。应该按照进度表进行硬件的预防性维护规程。

4.4 存储设备部分无法覆盖

如果介质在存储设备的一个地址段无法被覆盖（如磁盘驱动器无法使用的、“坏”的磁道或磁带的记录间隙）的情况下其释放就可能危及敏感数据的安全。例如，盘片使用中可能会形成无法使用的磁道或扇区，而以前可能有敏感数据被记录在这些区域。覆盖这些无法使用的磁道可能会很困难。在敏感信息被写入磁盘之前，应该辨别（标出）出所有无法使用的磁道、扇区或磁盘块。在磁盘的生命周期中，也应能够辨别更多的无法使用区域。如果发生了这种情况并且这些磁道无法被覆盖，敏感信息就可能被留在这些磁道上。在这种情况下，覆盖就不是可接受的净化方法，介质就应该被消磁或者消毁。

4.5 覆盖软件和清理

覆盖是清理数据的有效方法。在操作系统中，如果可以确信系统将系统资源与非受权用户相分离，那么就可以通过对未设定系统存储空间的覆盖完成数据清理。例如，文件（或所有系统存储器，如果情况许可）的单次覆盖就足以确保以前的信息无法通过键盘攻击得以重建。注意：简单地清除文件指针通常无法确保以前信息的不可恢复性。用于清理的软件应被置于严格的配置控制之下。这方面的附加信息参见《理

解受信系统中配置管理的指南》。［7］

4.6 覆盖软件和净化

国防部已经认可了用于净化数据的覆盖和消磁，但是不对每一个应用程序进行检查无法保证覆盖的效率。如果覆盖是被用于特定的应用程序，软件开发者的软件设计必须能确保软件对介质上所有的可寻址部分执行连续写入而无论中间发生了什么错误。所有可用扇区的这种错误都应该连同当前内容清单一起报告。另外，必须完全覆盖不可用扇区，因为不可用扇区清单无法显示扇区内是否包含任何敏感数据。如果在覆盖期间发生了任何错误或任何无法使用的扇区不能被覆盖,则要求进行消磁。

信任覆盖软件对磁盘进行净化还有其它一些风险。软件所运行的环境难以约束。因此，在软件开发过程在必须谨慎处理以确保软件不会被暗中破坏。覆盖软件的保护级别应该等同于其净化的介质的保护级别，必须对软件运行的操作系统和软件本身施行严格的配置控制。必须保护覆盖软件免遭非受权修改。［7］

4.7 合同义务

除非使用得到认可的规程撤销介质的密级，否则不能归还包含有非移动磁存储介质的租用设备。在获得担保维修服务或在租赁期结束归还设备时可能会遇到问题。合同维护协议应涉及到介质消磁及其对设备担保的影响方面的问题。

4.8 维护

正确的净化对于常规和非常规维护都特别重要。在非保证人员进行维护操作前应该执行净化规程并撤销设备的密级。如果净化不可行、过于昂贵，或可能损毁设备，则应该采取谨慎措施减少对设备上敏感信息的威胁。应该有得到指导的人员观察维护活动以辨别错误行动和防止非受权泄漏。

如果AIS上的测试和诊断（T & DE）没有被净化，T & DE就有可能捕获敏感信息。为防止非受权泄漏，应该在使用后对T & DE进行净化或按照AIS上驻留信息的最高级别对其进行保护。

例如，如果维护敏感的磁盘驱动器，陪同人员应该知道不允许维护人员将损坏磁盘从设施中取走。当维护人员更改设备的保护特性时陪同也应该有辨别能力。

4.9 数据敏感性

AIS存储介质可能包含有过于敏感的信息，这些AIS或其存储介质永远也不会被撤销密级。此类信息的例子是标有加密的通信安全（COMSEC）信息或单一综合性实施计划（SIOP）信息。这种情况下，介质的持有者除非在适当权威批准机构的指示下，

否则不应试图撤销介质的密级或释放介质。[9]消毁可能是清除如此高敏感介质存储的唯一选择。

4.10 消磁

虽然消磁是净化多数磁存储介质的最佳方法，但也不是没有风险的。例如，在消磁周期完成之前介质可能被拿走。消磁器也可能出现故障或随着使用年限的增长使性能有所降低。好的消磁器设计能够减少这些情况，但无法完全消除这些风险。这些风险可以通过定期测试予以消减（参见3.5节，“消磁设备故障”）。

错误地使用I型消磁器净化II型磁带是另一种风险。I型消磁器无法净化II型磁带。应该有标签贴在磁带的卷轴上以辨别介质的顽矫性，因为顽矫性无法完全通过物理外观来辨别。应该使用严格的物品清单控制措施确保能够辨别磁带的类型以保证净化规程的正确使用。如果使用了类型标签，除非将磁带从磁带卷上剪除或消毁磁带卷本身，否则不应清除类型标签。除非撤销介质的密级，否则显示安全级别的标签不应被清除。有关标签的更多信息参见3.3节，《标注磁带》。

5 标准

5.1 通用规程

有两种国防部政策允许的用于对曾经处理过敏感信息的AIS内存和第二存储器进行清理和净化的主要规程。[1]其它规程是介质特定的，本章将在适当的位置予以详细描述。当介质可用周期结束时需要被销毁。

5.1.1 覆盖

覆盖是将非保密数据写入以前存有敏感数据的存储位置的过程。为了满足国防部的清理需求，只要将任何字符写入所有所需的数据位置就可以了。为了净化AIS存储介质，国防部要求使用某种覆盖组合、然后是其补数组合，最后使用另一种组合；如先用0011 0101覆盖，接着用1100 1010，然后用1001 0111。覆盖必须完成的次数与存储介质有关，有时候与其敏感性有关，有时候因国防部门的需求有所不同。在任何情况下，直到使用非保密数据进行最后的覆盖后净化才算完成。

5.1.2 消磁

消磁是磁介质被擦除的过程，即还原到其最初的退磁状态。为满足国防部对保密磁带的消磁需求，消磁器必须符合第3章“消磁器”中讨论的测试需求。

5.1.3 销毁

在将介质提交销毁前对其进行净化是很好的措施。通常会使用以下方法之一来销毁介质。（虽然选项d和e是被认可的方法，但是它们使用酸液来清除记录表面，所以是危险和不必要的。建议使用选项a、b、c来取代d和e。）

a. 在得到认可的金属销毁设施中销毁，即熔炼、瓦解或粉碎。
b. 焚化。
c. 使用研磨剂（砂轮或圆片磨）对磁盘或磁鼓表面进行研磨。确保在废弃前完全清除整个记录表面。也要采取保护措施防止吸入研磨粉尘。
d. 使用浓缩氢碘酸（浓度55％到58％）溶解磁盘表面的三氧化二铁微粒。这种方法只能由专业人员在良好通风的环境中进行。
e. 使用酸活化剂 Dubais Race A (8010 181 7171)和剥离剂 Dubais Race B (8010 181 7170)处理磁鼓记录表面。然后使用工业丙酮(6810 184 4796)清除磁鼓表面的残余物。以上方法应该在通风良好的环境中进行，人员必须配戴眼罩。处理酸液时一定要非常小心。此过程只能由专业的得到批准的人员进行。

销毁技术和紧急销毁方面的更多信息参见国防分析协会（IDA）报告R-321，《信息存储介质的紧急销毁》。［6］

5.2 特殊规程

DoD 5200.28-M提供了用于对存储介质进行清理、净化、撤销密级和销毁的国防部规程。“标准”这一章体现了这些规程的一些内容但不提供完整的规程（如使用三次覆盖净化磁盘）。这是因为这些标准是不断发展变化的，而本文《理解自动化信息系统中数据残留的指南》不应被用做政策的替代品。

5.2.1 磁带

虽然覆盖可以被用作清理这种介质的方法，但是这种方法非常耗时通常不被使用。而且记录缝隙也不易被正确清理。使用I和II型消磁器是清理I、II、III型磁带较好方法。这种规程适用于清理，但并非适用于所有类型磁带的净化。

使用适当的消磁器进行消磁是国防部接受的净化这种介质的唯一办法。应该特别注意的是，I型消磁器只可以净化I型磁带，而II型消磁器可以净化I型和II型磁带。现在还没有符合NSA/CSS L14-4A规范的用于净化III型磁带的消磁器。

5.2.2 硬盘

国防部认可覆盖和消磁做为清除和净化这种介质的方法。更多的信息参见第4章“风险考虑因素”和DoD 5200.28-M。消磁后的磁盘通常需要恢复厂家预设的时间同步磁迹。I型消磁器和得到认可的手持式磁铁可以净化1100奥斯特以下顽矫性的这种介质。如果使用手持式磁铁，磁铁必须几乎直接接触磁盘，除了中间隔有一层防止划伤磁盘的保护片。有时有可能将磁铁插入盘片之间而无需拆卸。实际使用时，如果必须拆卸磁盘，通常销毁这些盘片比消磁后重新组装要容易。

最近完成的研究表明，消磁是净化硬盘介质的有效方法。箱式消磁设备可以用于擦除封装磁盘块和温氏硬盘驱动器而无需拆卸驱动器的盘片。在操作时必须小心避免磁盘驱动器被阻挡磁场的材料包裹。研究显示，温氏磁盘驱动器的铝质外壳会将磁场削弱2分贝。目前正在制定用于国防部的操作指导。

5.2.3 磁鼓

国防部认可覆盖和消磁做为清除和净化这种介质的方法。更多的信息参见第4章“风险考虑因素”和DoD 5200.28-M。I型消磁器和得到认可的手持式磁铁可以净化这种介质。不过后者只是实践中的一种备用选项。

5.2.4 软磁盘和磁卡

国防部认可覆盖做为清理而不是净化软磁盘的方法。消磁是首选的方法。磁卡技术已经过时不太常用了。使用I型消磁器或得到认可的手持式磁铁是国防部接受的用于净化任何顽矫性水平软盘和磁卡的唯一方法。更多信息参见DoD 5200.28-M。

5.2.5 磁芯存储器

国防部认可的清理和净化磁芯存储器的方法包括覆盖和消磁。更多信息参见DoD 5200.28-M。

5.2.6 磁膜线存储器

覆盖磁膜线存储器时存在与相同存储位置驻留信息时间长度相关的一些限制。更多信息参见DoD 5200.28-M。

5.2.7 薄片存储器

国防部认可覆盖和消磁做为清除和净化薄片存储器的方法。I型消磁器或得到认可的手持式磁铁可以净化这种介质。

5.2.8 磁泡存储器

国防部认可覆盖和消磁做为清除和净化磁泡存储器的方法。磁泡存储器单元被设计为具有内部偏压控制机制用于将内部偏压调整（即升高）到一定水平造成所有的磁泡崩溃，这可以作为一种可选的规程。一些磁泡设备可以通过发送z-coil脉冲进行芯片擦除。如果存储器被设计为使用偏压控制，供应商会提供足以导致所有磁泡崩溃的正确偏压值的信息。I型消磁器或得到认可的手持式磁铁可以净化这种介质。消磁后的磁泡通常需要使用厂商提供的程序进行再次初始化。磁泡存储器在使用任何此类的净化方法后没有被发现具有任何磁性残留。

5.2.9 随机存取存储器（RAM）

国防部认可覆盖和切断电源供应是清理和净化RAM的方法。更多信息参见DoD 5200.28-M。

5.2.10 只读存储器（ROM）

由于数据被永久性地存放在ROM中，所以清理和净化与这种介质无关。更多信息参见DoD 5200.28-M。

5.2.11 可擦除可编程只读存储器(UVPROM)

国防部认可使用紫外光线是清理和净化UVPROM的方法。更多信息参见DoD 5200.28-M。

5.2.12 电可擦除只读存储器(EEPROM)

国防部认可了多种形式（如单步芯片擦除、个别覆盖等）做为清理或净化EEPROM的方法。更多信息参见DoD 5200.28-M。

6 其它存储和覆盖技术

6.1 光盘

以下是光盘的例子：CD-ROM（只读）、WORM（一次写多次读）和磁光盘（多次读多次写）。目前，不存在被认为是足以确保净化这些介质的规程。磁光盘技术综合使用激光和磁技术获得远远超过单独使用磁技术所获得的磁盘数据密度。可以通过单次覆盖清理磁光盘，但是通过覆盖净化不被认为是足够的。

6.2 铁电随机存取存储器

此技术将磁技术与半导体随机存取存储器技术相结合在失去电源时获得数据保持能力。还没有发布任何规程来确保清理和净化这些介质。但是，与其它任何类型的存储介质一样，单次覆盖对于清理来说是足够的。

6.3 磁盘练习器

如前面4.6节“覆盖软件和净化”中提到的那样，使用覆盖软件净化磁盘存在很多缺点。其中一些缺点是缺乏具有专用操作系统的磁盘练习器。温氏驱动器厂商使用磁盘练习器来进行厂商需要的特殊操作。为了净化温氏驱动器，温氏单元必须被插入到磁盘练习器中。磁盘练习器能够写入磁盘任何部分而不管操作系统是否将其标注为不可用扇区。某些练习器还具有使用不同频率写入的能力。这使它们成为覆盖软件的有效选择，但是其净化磁盘的能力还没有经过测试。

7 未来的方向

进一步的研究可以使数据残留方面的多个领域受益。在确定覆盖能够正确地完成净化功能之后，就应该研究使用磁盘练习器进行磁盘净化。因为磁光盘使用的增长，也应该启动这种介质净化方面的研究。

Michael P. Sharrock撰写的《微粒磁记录：回顾》是关于磁盘和磁带的磁涂层技术方面不错的读本。［18］未来存储趋势方面的论文参见Mark H. Kryder在数据存储技术中的《2000年代数据存储趋势》。IEEE关于磁技术的学报提供了大量关于磁技术领域的信息，其中有关于AIS存储介质剩磁问题专业论述方面的专题。

有关箱式消磁器方面的公告会不断出现。在消磁器产品清单中查看这些公告以及有关磁介质消磁方面规定的公告。

需要对国防部政策、规程和指导进行不间断的调整才能够跟上不断变化的存储技术。虽然没有专门机构负责确保擦除标准的更新状态，但是有不少机构资助确保擦除标准能够提供足够安全级别方面的研究。这可能会造成重复劳动，但是也为以前的工作提供了附加验证。尽管如此，专门机构还是可以确保只有在需要的情况下才进行重复研究。随着存储技术的进步以及清理和净化规程的制定和修改，本指导方针将定期更新以反映这些变化。DoD 5200.28-M也应该被不断更新。

术语表

自动化信息系统

被设置用于收集、创建、交流、计算、分发、处理、存储和／或控制数据或信息的计算机硬件、固件和／或软件的组合。

AIS存储介质

被AS系统用于记录数据的物质。

清理AIS存储介质

在处理的结束阶段清除AIS中的敏感数据，包括AIS存储设备和其它具有存储能力的外设中的，这种方式提供与数据敏感性相当的保证，即无法使用普通的系统功能，也就是通过键盘重建数据。在清理前无需将AIS与外部网络断开。

顽矫力

为了将磁感应减少到零而施加的负的或反向磁力。

顽矫性

将磁感应减少到到零所需施加的磁场（反向）总量。通常用于表示磁介质可以被消磁的容易程度。

配置控制

在系统实施前、实施中和实施后对系统硬件、固件、软件和文档的修改进行控制，为防止将错误修改引入系统提供充分保证的过程。参照“配置管理”。

配置管理

通过在系统开发和运行生命周期中对系统硬件、软件、固件、文档、测试、测试装置和测试文档的更改进行控制的方式获得安全特性和保证的管理活动。参照“配置控制”。

数据

适于由人或AIS交流、解释或处理的事实、概念或指令的表示。

撤销AIS存储介质的密级

撤销相关介质保密级别的规程和管理决策。

消磁器

可以产生用于对磁介质消磁的磁场的设备。

消磁

通过施加反向磁场使磁感应减少到零。也被称为“去磁”。

消磁器产品清单（DPL）

符合国家安全局在参考资料13中发布的规范，出于商业目的生产的消磁器的清单。国家安全局将这个清单包含在其信息系统安全产品和服务目录中。

指定的批准机关（DAA）

有权决定AIS的安全保护措施是否可以接受的官员或可以负责发布记录有接受这些保护措施决策的审批意见的官员。DAA必须是具有评估AIS整体使命需求和为AIS开发者或拥有者提供关于AIS安全形势中风险方面的概念指导职权的机构成员。

降低密级

降低相关介质的保密级别的规程和管理决策。

擦除

清除存储介质上所记录数据的过程。

高斯

由磁力产生的磁通量密度的测量单位。

信息系统安全官（ISSO）

对DAA负责以确保在从系统的概念形成阶段到其设计、开发、运行、维护和安全废弃的整个生命周期中提供和实施安全保护的人。

信息系统安全产品和服务目录（INFOSEC目录）

由国家安全局每季度发布的旨在协助选择提供适当信息安全水平的产品和服务的目录。国家安全局在此出版物中发布DPL，此出版物可以通过政府的印刷机构获得。

记录间隙

磁带数据记录之间的“区域”。

键盘攻击

通过一般系统用户可获得的资源进行的数据提取，可以包括高级的软件诊断工具。

实验室攻击

通过精密设备的协助进行的数据提取。

磁场密度

创建期望磁通量所需的磁力，用H符号表示（参见“奥斯特”的定义）。

磁通量

表示磁场的磁力线。

磁通量密度

磁场力的表示，使用符号B表示（参见“高斯”的定义）。

剩磁

在取消所施加的磁场后磁路中所遗留的磁通量密度。为了便于论述，最好将剩磁描述为在介质擦除后遗留在磁介质上的残留信息。

磁饱和

增加磁力将不产生或只产生极小磁化的状态。

对象重用

将包含一个或多个对象的介质（如内存页面、磁盘扇区或磁带）重新设定给某些主体。为了进行安全的设定，应通过标准的系统机制防止新的主体获得以前所包含的残留数据。

奥斯特

磁场力的单位。

覆盖规程

通过在介质所存储的数据上记录非保密数据组合的方式消毁AIS存储介质记录的数据的规程。

永久磁铁消磁器

产生用于对磁存储介质进行消磁的磁场的手持式永久磁铁。

净化

在处理的结束阶段清除AIS中的敏感数据，包括AIS存储设备和其它具有存储能力的外设中的，这种方式提供与数据敏感性相当的保证，即无法使用末端开放的实验室技术重建数据。在执行净化前AIS必须与外部网络断开。

残留

存储介质在擦除后遗留的残余信息。

提取

通过搜索对象的残留(文件存储空间)获得非受权数据.

受信计算机系统评测标准（TCSEC）

由国家计算机安全中心发布的包含评估系统内建的硬件和软件安全控制效率保证水平的一系列统一的基本需求和评测级别的文件。这些标准被制定用于将处理和／或存储敏感或保密数据系统的设计和评测。此文件是DoD 5200.28-STD，通常也被称为标准或桔皮书。

受信计算基（TCB）

计算机系统内保护机制的总称，包括硬件、固件和软件，这些组合负责执行安全政策。TCB包括一个或多个组件一同对产品或系统执行统一的安全政策。TCB正确执行安全政策的能力仅依赖于TCB的内部机制以及系统管理人员输入与安全政策相关的正确参数（如用户许可证）。

受信计算系统

部署了足够的硬件和软件完整性措施，被允许用于同时处理一定范围内的敏感或保密信息的系统。

I型磁带

顽矫性不超过350奥特斯的磁带（也被称为低能量磁带）。

II型磁带

顽矫性在351和750奥特斯之间的磁带（也被称为高能量磁带）。

III型磁带

顽矫性在750奥特斯以上的磁带。

参考资料

[1] Automated Data Processing Security Manual, Department of Defense Manual, DoD 5200.28-M, January 1973 with change pages in June 1979 (now under revision).

[2] Care and Handling of Computer Magnetic Storage Media, Department of Commerce, National Bureau of Standards Special Publication 500-101, June 1983.

[3] Computer Security Evaluation Center, Department of Defense Directive, DoDD 5215.1,25 October 1982.

[4] Department of the Navy Automated Data Processing Security Program, Chief of Naval Operations Instruction, OPNAVINST 5239.1A with change 1, 3 August 1982.

[5] Department of the Navy Automated Information System Security Program, Secretary of the Navy Instruction, SECNAVINST 5239.2, 1 November 1989.

[6] "Emergency Destruction of Information Storing Media," Institute for Defense Analyses Report, R-321, December 1987.

[7] A Guide to Understanding Configuration Management in Trusted Systems, National Computer Security Center Technical Guideline, NCSC-TG-006, Version 1,28 March 1988.

[8] Industrial Security Manual for Safeguarding Classified Information, Department of Defense Manual, DoD 5220.22-M, June 1987.

[9] Information Systems Security, Army Regulation, AR 380-19, 4 September 1990.

[10] Information Systems Security Products and Services Catalogue, National Security Agency, quarterly publication.

[11] Katti, Romney R., "Erasure in Magnetic Recording Media," doctoral dissertation, Carnegie-Mellon University, 12 April 1988.

[12] Kryder, Mark H., "Data Storage in 2000-Trends in Data Storage Technologies," IEEE Transactions on Magnetics, Vol. 25, No. 6, November 1989.

[13] Magnetic Tape Degausser, National Security Agency/Central Security Service (NSA/CSS) Specification L1 4-4-A, 31 October 1985.

[14] Mountfield, K. R., and M. H. Kryder, "The Effect of Erasure in Particulate Disk Media," IEEE Transactions On Magnetics, Vol. 25, No. 5, September 1989.

[15] National Policy on Telecommunications and Automated Information Systems Security, National Security Decision Directive, NSDD 145, 17 September Page 26 1984.

[16] Remanence Security, Air Force Systems Security Instruction, AFSSI 5020,15 April 1991.

[17] Security Requirements for Automated Information Systems, Department of Defense Directive, DoDD 5200.28, March 1988.

[18] Sharrock, Michael P., "Particulate Magnetic Recording: A Review," IEEE Transactions on Magnetics, Vol. 25, No. 6, November 1989.

[19] "Signal Processing Applications Techniques to Magnetic Erasure Data," Illinois Institute of Technology, Research Institute, Final Reports for Projects E06522, K06005, and K06051, February 1982, September 1982, and March 1984 respectively.

[20] Trusted Computer System Evaluation Criteria, Department of Defense Standard, DoD 5200.28-STD, December 1985.

[21] Veeravalli, Venugopal V., "Detection of Digital Information From Erased Magnetic Disks," masters thesis, Carnegie-Mellon University, 1987.

[22] Wiesen, Kurt, "Modeling of Magnetic Media," masters thesis, Carnegie-Mellon University, July 1986.